Shamrock Consulting Group
707 Intrepid Way
Davidsonville, MD 21035
May 24, 2013

The Honorable John Gleeson
U.S. District Court for the Eastern District of New York
United States Courthouse
225 Cadman Plaza East
Brooklyn, New York 11201

12CR763

Dear Judge Gleeson:

Thank you for considering overturning the DPA with HSBC. As an anti-money laundering and financial crime specialist, it has been extremely frustrating to me to see financial institutions get away with only paying fines for their criminal behavior. In response to the HSBC agreement and the Permanent Subcommittee's 2012 report, I wrote an article for the Association of Certified Financial Crime Specialists called *Criminal Intent*. Here is the link: http://www.financialcrimeconference.com/wp-content/uploads/2012/09/marie-kerr-1.pdf; attached is a copy.

Perhaps my 12 years of Catholic school inform my abhorrence of letting the bad guys win. In any case, I believe we must prevent further moral hazard by not allowing criminal activity to go unpunished. DPAs seem to be the cost of doing business and the "lapses" continue.

In your position, I understand you will appoint a person to oversee the remediation of HSBC's poor controls, and that this individual will likely be an attorney. While this is important, I also believe oversight is needed of the many back-office functions and software applications that support the detection of money laundering and fraud. That is my specialty—for over 30 years. Please consider that a deep understanding of *how* things work is also important. I would gladly help, and I've enclosed my resume.

Thanks again for your courageous stand against egregious malfeasance by international financial institutions.

Respectfully,

Marie Kerr
Founder

CRIMINAL INTENT
A Consultant's Lament

To call recent bank transgressions "compliance failures" is an insult to those of us who work in the industry. Criminal intent is the only take-away from anyone, like me, who has worked in banking, anti-money laundering (AML), software creation, audit readiness, compliance and process engineering. Blaming "the system" is a typical excuse, as is "we need better training (of our low-level back-office staff)." No, as the HSBC report clearly shows, the bank knew exactly what it was doing. And it wasn't just skirting Bank Secrecy Act (BSA) or AML mandates, it *actively* helped run criminal enterprises by hiding their egregious transactions from scrutiny. HSBC isn't alone here; it shares the following modus operandi (MO) with a long list of financial institutions:

1. Wire stripping—data elements from wire transfers were removed before being sent on to other banks AND from the download sent to the detection/transaction monitoring system(s). The banks knowingly removed data that would identify banned countries or people. This effectively disabled the detection systems because what isn't captured isn't monitored.
2. Risk assessments—the bank assigned low-risk scores to countries and customers that did not pass the most rudimentary smell test. This also disabled the detection systems as risk scores are integral to analytic algorithms. Wire stripping + low-risk scores = junk from the detection system. OK, some structuring might be found, but money laundering, terrorist financing and tax evasion from KNOWN bad guys[1] would not.
3. Organizational bullying—despite pleas from people within the company who knew these things were wrong, they were: dismissed, ignored, reassigned.
4. Revolving door—an adjunct to organizational bullying. A "Who's on First" scorecard is always needed in megabanks, but these banks made keeping up with the scorecard next to impossible.
5. Temporary Organizational Units—ad-hoc groups such as committees, task forces and project teams can often serve to obfuscate. While they may be tasked with "figuring this mess out" they have no real authority and may be the dupes of the bank leaders.
6. Lax oversight—not the topic here, but significant in its enormity.
7. Consultants and more consultants—one of a consultant's mantras might be "you take the glory and I'll take the money," but when financial institutions are guilty of criminal intent, the bank's mantra becomes "you take the blame because you're the expert." Financial institutions whose crimes match the MO of HSBC were filled with big-name consultancies, experts in their field, unjustly maligned. Consultants were also shown the revolving door.

Because one of the topics of the International Financial Crime Conference & Exhibition[2] is "Guarding against the Enemy Within" I think it is only fair that we point to the willful

[1] Catch-all term for money launderers, terrorists and tax evaders.
[2] Annual conference of the Association of Financial Crime Specialists (ACFCS)

acts of C-Suite executives as the perpetrators of these egregious "lapses." The best process and IT controls are useless against a loss-of-job threat. If controls and their documentation are in all the right places—and that is possible—then only an override of the control(s) can explain the "lapse."

Overrides are cousins to "walk-throughs," something I discovered early in my career. A C-suite executive has an important client (or need) that has to be done NOW, so policies and procedures are pushed aside. This executive typically has employment power over all concerned and only needs to state a broad reason for the override. And the lower the level of the person performing the override, the less likely they are to speak up. Here's an example: C-Suite Guy asks a wires clerk to not enter certain data for international wires[3]. Perhaps the reason is "they're swamped, understaffed." The low-level person accepts this and no one is the wiser. Policies and procedures remain intact and an audit might only reveal that this back-office employee needs more training.

Detection systems are not rocket science, the concept of controls is not new nor is linking policies to procedures and documentation. Best practices for all of these things are common: anti-money laundering, project management, e-discovery, business process modeling, fraud examination, etc. Did all of these banks have "lapses" because of poor staffing? No, the regulations are clear (there's no ambiguity re bulk cash movement) and expertise abounds.

As a fraud/AML/IT specialist and a writer I would love to point out how these cases could have been avoided. But it's hard to make a case for controls, training, new systems, etc., when what I is see is gross misconduct and criminal intent—actions made by *people*. It's hard to guard against this level of "enemy within."

[3] Some wire data is still manually entered and these can be important fields for analyzing. Hidden codes, such as "FFC abcllc" might indicate that a company called ABC, LLC is the actual beneficiary. Or, "boo abcllc" could mean that the company is the actual originator. FFC means "for further credit; BOO means "by order of." There are more hidden but meaningful codes within free-text fields.

MARIE G. KERR, CFCS, PMP

707 Intrepid Way, Davidsonville, MD 21035 (410) 353-4414
mkerr@shamrockAML.com

EXECUTIVE SUMMARY

Financial industry veteran with a deep understanding of how financial institutions work, specializing in financial crime/fraud detection, anti-money laundering (AML), regulatory issues, compliance solutions, process design, data analytics, IT development/implementation. Practice includes both high-level advisory and hands-on expertise in the public and private sectors including:

- Risk analysis and mitigation
- Program development and project management
- Operational strategy development
- Vendor management, acquisition and competitive intelligence
- Gap and data analysis
- Forensic financial analysis

PROFESSIONAL EXPERIENCE

President **Shamrock Consulting Group**
2001 – Present **Washington, DC metro area**

Created consultancy offering unique competencies in technology, back/middle office, financial crime/fraud/AML detection and mitigation. Recent engagements include:

- *Litigation Support*—developed strategy and interrogatories for financial crime (fraud) case involving two large international banks;
- *Homeland Security Program Advisor and SME*—stood up a Know Your Customer (KYC)/Compliance/fraud detection program for a DHS program;
- *Bank Merger + Acquisition: IT and AML Advisor*—developed IT and AML integration plans for a three-bank merger;
- *Forensic AML "Look-back"*—member of a forensic AML investigation with a concentration on due diligence of parties and counterparties in wire transfer transactions;
- *AML Program Assessment and Development—International Gaming Company*—advised Mexico-based gaming company on their money laundering risks and mitigation strategies;
- *AML Product Assessment for Large Vendor*—created product strategy and competitive assessment for a major transaction monitoring vendor experiencing slowing sales;
- *AML Program and Risk Assessment*—assessed Bank Secrecy Act/AML compliance for a large mortgage financing company (now infamous);
- *Project Manager for AML Transaction Monitoring systems*—implemented several commercial off-the-shelf (COTS) AML transaction monitoring/ case management systems.

Program Manager **ACI Worldwide, New York, NY**
1997 – 2000

Project expert and champion for my Regulation E software creation, Claim*Track*, after the product was purchased by ACI. As Program Manager, exhibited product; created sales and marketing collateral; trained staff; and worked with other vendors to create new solutions using Claim*Track* as the base technology. Claim*Track* is still being sold by ACI under the name ACI Claims Manager.

Co-Founder and COO **Shamrock Systems Corporation, Crofton, MD**
1988 – 1997
Designed, developed, marketed and supported Claim*Track*, the first COTS product for debit card claims, adjustments, chargebacks and Regulation E compliance. The software included case management, fraud detection and compliance functionality; it was used by over 100 financial institutions worldwide, including Bank of America, Washington Mutual and Citibank. Responsible for identifying marketing venues, advertising strategy, functional enhancements and customer satisfaction. Sold the company and product to ACI Worldwide in 1997.

1979 – 1988 **Riggs Bank N.A., Washington, DC**
Vice President and Manager, Electronic Banking
Implemented technical infrastructure and processes for Riggs' entrance into regional and international debit card networks; member of networks' operating committees; member of American Bankers Association (ABA) conference development committees.
Assistant Vice President, Business Systems Analysis
Managed staff of internal consultants and Project Managers during period of rapid growth, organizational change and new technologies.

EDUCATION

Cornell University, BS, Economics
Kellogg School of Management, Northwestern University, 1 year of MBA coursework

DISTINCTIONS/CERTIFICATIONS/MEMBERSHIPS

Certified Financial Crime Specialist (CFCS)
Certified Anti-Money Laundering Specialist (CAMS)
Certified Project Management Professional (PMP)
Cornell Alumni Admissions Ambassador Network (CAAAN)

PUBLICATIONS (Partial List)

- *Criminal Intent,* Association of Certified Financial Crime Specialists (ACFCS), 2012
- *Anatomy of Financial Crime through the Lens of IT Systems,* ACFCS webinar, 2012
- *How Back Office Processes can sabotage even the best Transaction Monitoring Systems,* Money Laundering Alert, June, 2007
- *The Infrastructure of Compliance—Building a Bridge to Vendor BSA/AML Solutions,* Money Laundering Alert conference paper, 2005
- *It's All about the Data,* ACAMS Anti-Money Laundering Technology Resource Directory, 2003-2004

SPEAKING ENGAGEMENTS (Partial List)

- **ACFCS International Financial Crime Conference**, 2012
- **10th and 12th Annual International Money Laundering Conference & Exhibition,** 2005 and 2007; Featured Speaker in 2007
- **Financial Markets World:** *AML in the Securities and Investments Industries*, 2005